MICHAEL R. REESE (Cal. SBN 206773)
mreese@reesellp.com
SUE J. NAM (Cal. SBN 206729)
snam@reesellp.com
REESE LLP
100 West 93rd Street, 16th Floor
New York, New York 10025
Telephone: (212) 643-0500

GEORGE V. GRANADE (Cal. SBN 316050)
ggranade@reesellp.com
REESE LLP
8484 Wilshire Boulevard, Suite 515
Los Angeles, California 90211
Telephone: (310) 393-0070

CHARLES D. MOORE (admitted *pro hac vice*)
cmoore@reesellp.com
REESE LLP
100 South 5th Street, Suite 1900
Minneapolis, Minnesota 55402
Telephone: (212) 643-0500

KEVIN LAUKAITIS (*pro hac vice* pending)
klaukaitis@laukaitislaw.com
LAUKAITIS LAW FIRM LLC
737 Bainbridge Street, Suite 155
Philadelphia, Pennsylvania 19147
Telephone: (215) 789-4462

BRIAN C. GUDMUNDSON (admitted *pro hac vice*)
brian.gudmundson@zimmreed.com
RACHEL K. TACK (admitted *pro hac vice*)
rachel.tack@zimmreed.com
MICHAEL J. LAIRD (admitted *pro hac vice*)
michael.laird@zimmreed.com
ZIMMERMAN REED LLP
1100 IDS Center
80 South 8th Street
Minneapolis, Minnesota 55402
Telephone: (612) 341-0400

Attorneys for Plaintiff Joshua Keller and the Proposed Class

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

JOSHUA KELLER, on behalf of himself and all others similarly situated, Plaintiff, v. CHEGG, INC., Defendant.	CASE NO.: 3:22-cv-06986-JD **FIRST AMENDED COMPLAINT** **CLASS ACTION** **Jury Trial Demanded**

Plaintiff Joshua Keller ("Plaintiff"), by his undersigned counsel, files this First Amended Class Action Complaint on behalf of himself and a class of all similarly situated persons against Defendant Chegg, Inc. ("Chegg" or "Defendant"). Plaintiff bases the allegations below upon personal knowledge, information and belief, and the investigation of counsel, and states the following:

INTRODUCTION

1. Chegg is a multi-billion-dollar corporation that markets and sells direct-to-student educational products and services throughout the United States.[1] This includes renting textbooks, guiding customers in their search for scholarships, and offering online tutoring.[2] Chegg is the industry leader in the educational product and service space, and it holds itself out as a company consumers can trust. For example, Chegg claims it "strive[s] to improve the overall return on investment in education by helping students learn more in less time and at a lower cost."[3] The company also claims to bring "integrity to [its] products, customers, work environment, and the community."[4] According to Chegg, the target audience for its services and products is primarily high school and college students.[5]

2. Unfortunately for Chegg's customers, including Plaintiff and the Class[6] members, the company broke that trust and failed to safeguard the sensitive personal information of millions of individuals throughout the United States.

3. Chegg experienced a remarkable ***four*** data breaches in only a six-year span.

4. Since September 2017, the four Chegg data breaches occurred in or around the following dates: (1) September 2017; (2) April 2018; (3) April 2019; and (4) April 2020 (collectively, the "Data Breaches").

[1] *Multiple data breaches suggest ed tech company Chegg didn't do its homework, alleges FTC*, Leslie Fair, Federal Trade Commission, Oct. 31, 2022: https://www.ftc.gov/business-guidance/blog/2022/10/multiple-data-breaches-suggest-ed-tech-company-chegg-didnt-do-its-homework-alleges-ftc (last visited Nov. 4, 2022).
[2] *Id.*
[3] *Id.*
[4] *Id.*
[5] https://www.chegg.com/about/what-we-do/.
[6] "Class" is defined below.

5. It all started in 2016. After going public in 2013 due to increasing competition from Amazon, Chegg's stock sunk from an initial $12.50 to a low of $4 in early 2016.[7]

6. This is when Chegg's CEO, Dan Rosensweig, experienced great frustration, both personally and professionally, at Chegg. In a 2017 interview, Mr. Rosensweig said of this period:

> "You live in Silicon Valley, and everybody is a billionaire, and you're not. Everybody goes public and at least has the one moment where their stock goes up—and yours didn't. . . . I had a moment of sucking my thumb in bed."[8]

7. Rosensweig and Chegg knew they had to expand Chegg to increase profits. According to Chegg's 10-Q dated November 7, 2016, Chegg acknowledged the importance of expansion:

> We have expanded rapidly since we launched our online print textbook rental service in 2007. We anticipate further expanding our operations to offer additional products, services and content to help grow our student user base and to take advantage of favorable market opportunities. As we grow, our operations and the technology infrastructure we use to manage and account for our operations will become more complex, and managing these aspects of our business will become more challenging. Any future expansion will likely place significant demands on our resources, capabilities and systems, and we may need to develop new processes and procedures and expand the size of our infrastructure to respond to these demands.[9]

8. While Chegg certainly had a plan in place for expansion, the company also recognized the importance of data security, especially given the threat of hacking posed by students – who are Chegg's target market:

> Computer malware, viruses, physical or electronic break-ins and similar disruptions could lead to interruptions and delays in our services and operations and loss, misuse or theft of data. Computer malware, viruses, computer hacking and phishing attacks against online networking platforms have become more prevalent and may occur on our systems in the future. ***We believe that we could be a target for such attacks because of the incidence of hacking among students.***[10]

9. Despite Chegg's knowledge that it could be a target of a data breach, the company still failed to safeguard the sensitive information contained in its systems.

10. Chegg chose to focus on expanding its business and increasing profits while ignoring and neglecting the security of its system.

---

[7] https://www.forbes.com/sites/susanadams/2021/01/28/this-12-billion-company-is-getting-rich-off-students-cheating-their-way-through-covid/?sh=1ba7aa29363f.
[8] *Id.*
[9] https://d18rn0p25nwr6d.cloudfront.net/CIK-0001364954/f70a1c9d-576d-4ed8-a306-ba2c2d3cc3ea.pdf at p. 39.
[10] *Id.* at 43 (emphasis added).

11. So, while Chegg's stock price climbed to $11 in 2017 (nearly tripling from the previous year), Chegg experienced its first data breach.

12. The first data breach occurred in September 2017, when multiple Chegg employees fell for a phishing attack that allowed a hacker to gain access to employees' direct deposit information. Upon information and belief, this breach was limited to the exposure of employee data.

13. Approximately seven months later, in April 2018, a former Chegg contractor used login information the company shared with employees and contractors to access one of Chegg's third-party cloud databases, resulting in the exposure of millions of customers' personal information. According to the Federal Trade Commission ("FTC"), Chegg allowed employees and third-party contractors to access Amazon-hosted storage with a single access key that provided full administrative privileges over all information.[11] The April 2018 data breach exposed the personal information of approximately forty (40) million customers. The exposed personal information included names, email addresses, passwords, and for certain users, sensitive scholarship information such as dates of birth, parents' income range, sexual orientation, and disabilities. Upon information and belief, this breach exposed both consumer and employee data.

14. In September 2018, a threat intelligence vendor informed Chegg that a file containing some of the exfiltrated information from the April 2018 breach was available in an online forum.[12] Chegg reviewed the file as part of its own investigation, finding it held, among other things, approximately 25 million of the exfiltrated customers' passwords in plain text, meaning the threat actors had cracked the hash for those passwords.[13] Chegg required approximately 40 million Chegg platform users to reset their passwords.[14] Even after this, Chegg continued to store consumer personal information in plain text.[15]

---

[11] *FTC schools edtech giant Chegg over 'careless' cybersecurity practices*, Carly Page, Join TechCrunch+, Nov. 1, 2022: https://techcrunch.com/2022/11/01/ftc-chegg-breaches-cybersecurity/, (last visited Nov. 7, 2022).

[12] *In the Matter of CHEGG, INC., a corporation*, https://www.ftc.gov/system/files/ftc_gov/pdf/2023151-Chegg-Complaint.pdf (last visited Nov. 7, 2022).

[13] *Id.*

[14] *Id.*

[15] *Id.*

15. The third breach, in April 2019, was the result of another phishing attack, giving hackers access to a Chegg executive's email inbox, which contained personal information of Chegg users and employees, including financial and medical data.[16] Upon information and belief, this breach exposed both consumer and employee data.

16. And most recently, the fourth data breach in April 2020 exposed W-2 information, including birth dates and Social Security numbers, for approximately 700 current and former employees.[17] Upon information and belief, this data breach was limited to the exposure of employee data.

17. From September 2017 through April 2020, Chegg did not make reasonable modifications to its data security, including an egregious failure to implement any phishing attack training for its employees. It also did not implement a written data security policy until January 2021.[18]

18. On October 31, 2022, the FTC issued a proposed administrative complaint accusing Chegg of numerous cybersecurity lapses that resulted in the four data breaches between 2017 and 2020.[19]

19. In a press release published on the same day, the FTC announced it was taking action against Chegg "for its lax data security practices that exposed sensitive information about millions of its customers and employees, including Social Security numbers, email addresses and passwords."[20] The press release quoted the Director of FTC's Bureau of Consumer Protection as saying, "Chegg took shortcuts with millions of students' sensitive information."[21]

20. According to the FTC, the Data Breaches described above were the result of "poor data security practices," including a lack of multifactor authentication measures for employees to use to log on to Chegg's third-party databases; the use by employees and contractors of a single root level login for Chegg's third-party databases; Chegg's failure to monitor its network and databases for threats; the

---

[16] *Id.*
[17] *Id.*
[18] *In re Chegg, Inc.*, FTC File No. 202-3151 (Oct. 31, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/2023151-Chegg-Complaint.pdf, at ¶ 9.
[19] *FTC schools edtech giant Chegg over 'careless' cybersecurity practices*, *supra* note 11.
[20] FED. TRADE COMM'N, *FTC Brings Action Against Ed Tech Provider Chegg for Careless Security that Exposed Personal Data of Millions of Customers* (Oct. 31, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/10/ftc-brings-action-against-ed-tech-provider-chegg-careless-security-exposed-personal-data-millions.
[21] *Id.*

storing of users' and employees' data on Chegg's cloud storage databases in plain text; and Chegg's use until at least 2018 of outdated and weak encryption to protect user passwords.[22] Chegg thus failed to use "commercially reasonable security measures" to protect the personal information it collected and stored.[23]

21. Furthermore, the FTC pointed out that even after experiencing three phishing attacks, Chegg still continued to fail to provide adequate security training to employees and contractors, and it failed to implement a written security policy until January 2021.[24]

22. The FTC complaint noted that "because people often use the same email addresses and passwords for multiple accounts, exposure of such user credentials open users up to additional attacks by threat actors, including credential stuffing attacks," which occur "when a threat actor uses stolen credentials from one website to access user accounts on a different website."[25] Thus, a threat actor could use an email address and cracked password obtained from Chegg to attempt to access a user's financial accounts on other websites.[26]

23. The FTC complaint also states that "[e]ven if identity theft and fraud do not occur immediately after a breach, a breach of personal information such as that stored in Chegg's system makes identity theft and fraud more likely in the future,"[27] and "due to Chegg's failure to appropriately monitor its systems and lack of access controls and authentication protections for its [] databases, users' and employees' personal information, including health information and financial information, may have been exposed in other instances—beyond the [Data Breaches]—without Chegg's knowledge."[28]

24. According to the FTC complaint, Chegg users "had no way to know about Chegg's information security shortcomings,"[29] yet Chegg "could have prevented or mitigated these information security failures through readily available, and relatively low-cost, measures."[30]

---

[22] *Id.*
[23] *Id.*
[24] *Id.*
[25] *In re Chegg, Inc.*, FTC File No. 202-3151 (Oct. 31, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/2023151-Chegg-Complaint.pdf, at ¶ 19.
[26] *Id.*
[27] *Id.* at ¶ 20.
[28] *Id.* at ¶ 21.
[29] *Id.* as ¶ 22.
[30] *Id.* at ¶ 23.

25. On October 31, 2022, the FTC also publicized for public comment a proposed Decision and Order that would, among other things, "require[] [Chegg] to bolster its data security, limit the data the company can collect and retain, offer users multifactor authentication to secure their accounts, and allow users to access and delete their data."[31] The Decision and Order was associated with a consent agreement between the FTC and Chegg.[32]

26. On January 25, 2023, after receiving only one substantive comment about the proposed Decision and Order, the FTC voted 4-0 to finalize the Decision and Order against Chegg and send a letter to the commenter.[33]

27. On January 27, 2023, the FTC issued a press release reiterating that Chegg's data security had been "lax" and "careless" and that "[a]s a result of its poor data security, Chegg experienced four data breaches that exposed the personal information of about 40 million users and employees, including users' email addresses and sensitive scholarship data such as their dates of birth, sexual orientation and disabilities, as well as financial and medical information about Chegg employees."[34]

28. The press release explained that the final Decision and Order "requires Chegg to implement a comprehensive information security program, limit the data the company can collect and retain, offer users multifactor authentication to secure their accounts, and allow users to request access

[31] FED. TRADE COMM'N, *FTC Brings Action Against Ed Tech Provider Chegg for Careless Security that Exposed Personal Data of Millions of Customers* (Oct. 31, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/10/ftc-brings-action-against-ed-tech-provider-chegg-careless-security-exposed-personal-data-millions; Proposed Decision and Order, *In re Chegg, Inc.*, FTC File No. 202-3151 (Oct. 31, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/2023151-Chegg-Decision-and-Order.pdf; *see also* FED. TRADE COMM'N, *Analysis of Proposed Consent Order to Aid Public Comment In the Matter of Chegg, Inc., File No. 2023151* (Oct. 31, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/2023151-Chegg-Analysis-of-Proposed-Consent-Order-to-Aid-Public-Comment.pdf.

[32] *See* Agreement Containing Consent Order, *In re Chegg, Inc.*, FTC File No. 202-3151 (Oct. 31, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/2023151-Chegg-Agreement-Containing-Consent-Order.pdf.

[33] FED. TRADE COMM'N, *FTC Finalizes Order with Ed Tech Provider Chegg for Lax Security that Exposed Student Data* (Jan. 27, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/01/ftc-finalizes-order-ed-tech-provider-chegg-lax-security-exposed-student-data; Decision and Order, *In re Chegg, Inc.*, FTC Docket No. C-4782 (Jan. 25, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/Chegg-DecisionandOrder.pdf.

[34] FED. TRADE COMM'N, *FTC Finalizes Order with Ed Tech Provider Chegg for Lax Security that Exposed Student Data* (Jan. 27, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/01/ftc-finalizes-order-ed-tech-provider-chegg-lax-security-exposed-student-data.

to and deletion of their data."[35]

29. Chegg's ongoing failure to implement basic data security practices violates standard commercial practice, is wholly unreasonable, and caused harm to Plaintiff and the proposed Class of individuals impacted by the several Data Breaches.

30. Plaintiff therefore brings this First Amended Class Action Complaint seeking relief for his injuries and those of persons who were similarly impacted by the Data Breaches and Chegg's inadequate data security.

JURISDICTION

31. This Court has subject matter jurisdiction over this case pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005. Subject matter jurisdiction is proper because: (1) the amount in controversy in this class action exceeds five million dollars ($5,000,000), excluding interest and costs; (2) there are more than 100 Class members; (3) at least one member of the Class is diverse from the Defendants; and (4) the Defendant is not a government entity.

32. This Court has general personal jurisdiction over Chegg because Chegg is headquartered and operates its principal place of business in Santa Clara, California. Chegg has minimum contacts with California because it is located here and conducts substantial business here, and Plaintiff's claims arise from Chegg's conduct in California.

33. This Court is the proper venue for this case pursuant to 28 U.S.C. § 1391(a) and (b) because a substantial part of the events and omissions giving rise to Plaintiff's claims occurred in California and because Chegg conducts a substantial part of its business within this District.

[35] *Id.*

PARTIES

34. **Plaintiff** Joshua Keller is a resident and citizen of California residing in Hillsborough, California. Plaintiff has been a Chegg customer since approximately 2014 or 2015, at which time Mr. Keller was around fifteen years old. This means that when Mr. Keller originally became a Chegg customer, he was a minor, high school student, like many of Chegg's customers. Plaintiff was not presented with a Terms of Use from Chegg and does not recall reviewing any such terms upon signing up with Chegg or at any point thereafter. He used Chegg's services throughout his high school and college education, including for exam, homework, and project help.

35. In order to use Chegg's services, Mr. Keller and all users are required to provide their name, contact information, including email, username, passwords (which he likely repeated for other websites and/or applications), phone number and address, financial and payment information, including bank card information, date of birth, and other personal and sensitive information related to his education.

36. Plaintiff Keller trusted Chegg to protect and safeguard his personal identifiable information ("PII"), especially because Chegg is in the business of providing goods and services to students, who are vulnerable to cybersecurity attacks.

37. During the 2018 Data Breach, Plaintiff Keller was a Chegg customer, and Mr. Keller's PII remained in Chegg's databases and systems at this time. As such, Plaintiff was one of millions whose PII was hacked in the 2018 Data Breach.

38. Plaintiff reasonably believes his data was compromised by the Chegg Data Breaches and attributes the fraud and identity theft he has experienced to the 2018 Chegg Data Breach. After the Chegg Data Breaches, Plaintiff experienced identity theft and fraud, including multiple credit checks initiated on his behalf and a credit card issued in his name, both without his authorization, permission or consent. Specifically, in or around October 2022, Mr. Keller received multiple emails from his bank informing him that his identity had been stolen, including two credit inquiries initiated in his name with Capital One and Discover, and that a new Discover credit card was opened in his name.

39. Plaintiff Keller keeps, and has kept at all relevant times, his data secure through credit monitoring services and not unnecessarily sharing his data. As a direct result of the Chegg Data

Breaches, Plaintiff has spent time and effort with his bank dealing with this credit card fraud and identity theft. Mr. Keller also noticed an increase in spam calls and emails and spent time and effort changing multiple passwords to his various subscriptions or accounts. Plaintiff reasonably believes that all of this, the identity theft and fraud and the increase in spam, is a direct and proximate result of the Chegg Data Breaches, particularly because this fraud all occurred after the Data Breach, and Plaintiff does not reasonably believe it could be related to any other event. Additionally, Mr. Keller, to his knowledge, has not been the victim of any other data breaches and has not had any identity theft or fraud prior to what he experienced in October 2022, after his data was exposed by the Chegg Data Breaches.

40. Chegg never sent Mr. Keller a notice about any of the Chegg Data Breaches. Rather, Mr. Keller began investigating potential sources of his identity theft and fraud after October 2022. During that investigation, Mr. Keller found information about the Chegg Data Breaches and reasonably determined, based upon the available information, that the Chegg Data Breach caused his injuries and damages.

41. **Defendant** Chegg is a Delaware corporation with its headquarters and principal place of businesses in Santa Clara, California.

42. On information and belief, all digital interactions with Chegg occur via its servers in California.

43. On information and belief, all transactions with Chegg are completed via its servers in California.

BACKGROUND

A. Chegg Collects Sensitive Information from Users

44. In providing its services and for employment, Chegg requires and collects sensitive personal information from customers. This information includes name, email address, username, password, demographic, school, gender, age or birthdate, zip or postal code, photographs, information about academic and work history, phone number, mailing address, and information about interests and preferences.[36]

[36] *Privacy Policy*, https://www.chegg.com/en-US/privacypolicy (last visited Nov. 7, 2022).

45. If a user requests information about Chegg's scholarship services, the user is directed to update their profile. The additional information Chegg collects here includes a customer's religious denomination, heritage, date of birth, parents' income range, sexual orientation, military affiliations, citizenships, disabilities, interests, and participation in clubs and sports (collectively, the "Scholarship Search Data").[37] This data is highly sensitive.

46. As another example, in connection with its online tutoring services, Chegg records videos of tutoring sessions that include Chegg users' likeness, images, and voices. Again, this is highly sensitive information.

47. Chegg also collects information automatically when users use the services, including internet protocol (IP) address, user setting, MAC address, cookie identifiers, mobile carrier mobile advertising and other unique identifiers, details about the users' browsers, operating systems or devices, location information, Internet or mobile service provider, pages that users visit before, during, and after using the services, information about links users click, and other information about how users use Chegg's services.[38]

48. Taken together, the preceding four paragraphs, collectively and independently, identify "Sensitive Information."

B. The Process for Creating a Chegg Account

49. To create an account with Chegg on Defendant's website, chegg.com, a website user is prompted to input his email address and create a password, or use existing credentials he has with Apple, Facebook, or Google.[39]

50. After a user inputs an email address and password, they are prompted to answer the question: "Are you a student or parent?"[40]

51. If the user selects "student," two additional prompts appear, asking the student whether they are studying in "high school" or "college." If the student answers "high school," they are prompted to answer what year they plan to graduate. If the student answers "college," they are asked to "enter [a]

[37] *Profile Info*, https://www.chegg.com/my/profile (last visited, Nov. 7, 2022).
[38] *Privacy Policy*, *supra* note 36.
[39] https://www.chegg.com/auth?action=login&redirect=https%3A%2F%2Fwww.chegg.com%2F.
[40] *Id.*

college name." Users are not required to be 18 to create and use their own account, and a significant portion of the Chegg users were not 18 at the time they signed up with Chegg.

52. After inputting the information Chegg requests, the user can click the "Create account" button. Underneath the "Create an Account" submission button, and in smaller print than the rest of the text on the screen, it reads, "We respect your privacy. By clicking 'Create account' you agree to the Terms of Use and Privacy Policy."[41] The user is not required to click on the Terms of Use or Privacy Policy to create the account, and the Terms of Use and Privacy Policies are not reasonably presented to users. After an account is created, the user can input additional personal details into their profile and enter and save payment information.

53. If, by chance, the user reads beyond the "Create account" submission button before they create their account, and finds the option to click on the "Terms of Use" and does in fact click on those Terms (which they are not required to do to create an account) they can review the Terms of Use, last updated on June 29, 2021.[42]

C. Chegg's Services

54. According to Chegg's website, its prices start at $15.95 per month, and users can cancel any time.[43]

55. Chegg also offers textbooks for rent and sale, for which it touts students can save upwards of 90% compared to other textbook sellers.[44]

56. Chegg's services for students primarily include Chegg Study, Chegg Writing, Chegg Math Solver, Mathway, Chegg Study Pack, Busuu, and Thinkful.[45]

57. The Chegg Study subscription service provides "Expert Questions and Answers" and step-by-step "Textbook Solutions," helping students with their course work. When students need writing help, including plagiarism detection scans and creating citations for their papers, they can use the Chegg

[41] *Id.*
[42] https://www.chegg.com/en-US/termsofuse.
[43] https://www.chegg.com/.
[44] https://www.chegg.com/textbooks/.
[45] Chegg Quarterly Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934, Form 10-Q, Sept. 30, 2022, https://www.streetinsider.com/dr/news.php?id=20779210.

Writing subscription service.[46]

58. The Chegg Math Solver and Mathway subscription services help students understand math by providing a step-by-step math solver and calculator.[47]

59. Chegg Study Pack is a premium subscription bundle of Chegg Study, Chegg Writing, and Chegg Math Solver services, which also includes additional features such as flashcards, concept videos, practice questions and quizzes, and instructor-created materials from Chegg's "Uversity,"[48] which is "a platform for educators and faculty to share their education content with millions of learners on Chegg to help support their studies and enhance learner outcomes."[49]

60. The Thinkful skills-based learning platform offers professional courses focused on the most in-demand technology skills.[50]

61. Chegg's "Required Materials" include Chegg's print textbook and eTextbook offerings, which help students save money compared to the cost of buying new. Chegg has an extensive print textbook library primarily for rent and also for sale through Chegg's print textbook partners. Chegg also touts students can save upwards of 90% compared to other textbook rentals.[51]

62. During the nine months ending September 30, 2022, Chegg generated revenue of $561.7 million.

D. Chegg's Terms of Use

63. The Chegg Terms of Use ("Terms") contain the following statements[52]:

- "These [Terms] apply to the websites, mobile apps, applications and other interactive features or services that post a link to these Terms of Use (each, a 'Service' and collectively, the 'Services' or 'Chegg Websites')."
- "These [Terms] govern your use of the Services, regardless of how you access them, whether by

[46] *Id.*
[47] *Id.*
[48] *Id.*
[49] Business Wire, *Chegg announces "Uversity": A Creator Community for Educators* (June 2, 2021), https://www.businesswire.com/news/home/20210602006034/en/Chegg-announces-%E2%80%9CUversity%E2%80%9D-A-Creator-Community-for-Educators.
[50] Chegg Quarterly Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934, Form 10-Q, Sept. 30, 2022, https://www.streetinsider.com/dr/news.php?id=20779210.
[51] https://www.chegg.com/textbooks/.
[52] https://www.chegg.com/en-US/termsofuse.

computer, mobile device, or otherwise; and whether directly through our Services, or through any third-party website that links to them ('Linked Services'), and regardless of whether you are a registered user or a guest."

- "By clicking 'I Accept' or by using the Services, you agree to the [Terms]." There is not an "I Accept" prompt or option to click on the Terms page.
- "Arbitration Notice: Unless you opt out of arbitration within 30 days of the date you first agree to these terms of use by the following opt-out procedure specified in the 'dispute resolution' section below, and except where prohibited by local law or for certain types of disputes described in the 'dispute resolution' section below, you agree that disputes between you and Chegg will be resolved by binding, individual arbitration and you waive your right to participate in a class action lawsuit or class-wide arbitration."
- Plaintiff, like many of Chegg's customers began using Chegg's services or products as minors, and the 30 day opt-out period would have expired while they were still minors. Under the Terms, they do not receive another opportunity to opt out as an adult: "Chegg's updates to the 'Dispute Resolution', 'Class Action Waiver', 'Informal Dispute Resolution', and arbitration sections do not provide you with a new opportunity to opt out of the Arbitration Agreement if you have previously agreed to a version of the Terms of Use and did not validly opt out of arbitration."
- The arbitration provision, however, only purports to apply to disputes arising out of the Terms and the Services, as defined by the Terms. Specifically, the Terms state arbitration applies to a "dispute, claim or controversy between us arising out of or related to the Terms of Use or breach, termination, enforcement, interpretation, or validity thereof, of the Services or your use of the Services . . . ." It does not apply to disputes concerning Chegg's breach of legal duties existing outside of the agreement, including, as here, breaches of its legal obligations to reasonable secure customer data.
- The Terms also contain a statement that "Chegg provides a variety of services, both online and offline." Services here is not capitalized, like the defined Services within the Terms, and implicates services outside of those defined Services in the Terms, including those offered offline.

- Similarly, the Terms of Use alters individual's arbitration rights depending where other users have substantially similar claims. Specifically, the Terms of Use states that "in the event that there are 100 or more individual Requests of a similar nature filed against Chegg by or with the assistance of the same law firm, group of law firms or organizations within a 30 day period (or otherwise in close proximity), the AAA (1) will administer the arbitration demands in batches of 100 Requests per batch . . . ; (2) appoint one arbitrator for each batch; and (3) provide for the resolution of each batch as a single consolidated arbitration with one set of case management fees and arbitrator compensation due per batch, one procedural calendar, one hearing (if any) in a place to be determined by the arbitration, and one final award . . . ." Under the agreement, therefore, individuals' purported arbitration rights are altered by the presence of other similar claims and by the identity of their legal representatives.
- The Terms also purport to limit the availability of injunctive relief. On one hand, the Terms allow for injunctive relief for some user rights' violations: "Each party reserves the right to seek injunctive or other equitable relief in a court of competent jurisdiction with respect to any dispute related to the actual or threatened infringement, misappropriation or violation of a party's intellectual property or proprietary rights or breach of the User Content and Activities provisions of this Agreement." However, the Terms limit injunctive relief elsewhere, specifically, allowing "declaratory or injunctive relief only in favor of the individual party seeking relief and only to the extent necessary to provide relief warranted by the party's individual claim." Moreover, the Terms state that "in the event you suffer any damages, losses or injuries . . . the damages, if any, caused to you are not irreparable or sufficient to you to entitle you to an injunction . . . ."

E. Chegg's Privacy Policy

64. Chegg also has a Privacy Policy that has the following provisions[53]:

- "We at Chegg, Inc. ('Chegg') have created this privacy policy (the 'Privacy Policy') to describe our practices and your choices regarding information we collect through our websites, apps, mobile features, and other services that post a link to this Privacy Policy ('Service' or 'Services'),

[53] *Privacy Policy*, *supra* note 36.

as well as offline sources that may then be combined in our databases." Chegg includes the offline data it collects, which it does not include in the defined Services it provides, into its Privacy Policy.

- "We consider information that identifies you as a specific, identified individual to be personal information (such as your name and email address), and we treat additional information, including IP addresses and online identifiers, as personal information where required by applicable law."
- "In the course of using our Services, you may provide us with certain information, including contact information (such as your name, email address, telephone number, and social media user name); account information (such as your profile picture and birthday); payment and financial information; educational information (such as your school and year of graduation); demographic information (such as your gender, race, eligibility to work in the United States, and work history); information about your interests and preferences (such as your career goals, academic interests and clubs or sports you participate in)."
- "When you use our Services, we, our third-party service providers, and our business partners may automatically collect certain information ('Usage Information'). One of the ways we collect Usage Information is when you visit portions of our Services, our servers automatically generate logs to help us determine how people navigate through our Services, the content you access, and other interactions you may have with our Services."
- "We may not be able to provide you with access to some or all of our Services if you do not provide us with the requested information, (including, for example, personalization features, relevant advertisements, and special promotions)."
- "We implement commercially reasonable security measures to protect the security of your information."

F. Chegg's Inadequate Data Security Measures Exposed Customers' Sensitive Information

65. As part of its information technology infrastructure, Chegg uses a third-party service provided by Amazon Web Services called the Simple Storage Service ("S3"). S3 is a scalable cloud storage service that can be used to store and retrieve large amounts of data. The S3 stores data inside

virtual containers, called "buckets," against which individual access controls can be applied.[54]

66. Chegg relies on S3 buckets to store a wide variety of files that contain customers' sensitive personal information, including their names, passwords, dates of birth, and Scholarship Search Data.[55]

67. From at least 2017 to the 2020, Chegg has engaged in several practices that failed to provide reasonable security to prevent unauthorized access to customers' personal information. Among other things, Chegg:

a) failed to implement reasonable access controls to safeguard users' personal information stored in S3 databases until at least October 2018. Specifically, Chegg:

   i) failed to require employees and third-party contractors that access the S3 databases to use distinct access keys, instead permitting employees and contractors to use a single AWS access key that provided full administrative privileges over all data in the S3 databases ("AWS Root Credentials");

   ii) failed to restrict access to systems based on employees' or contractors' job functions;

   iii) failed to require multi-factor authentication for account access to the S3 databases; and

   iv) failed to rotate access keys to the S3 databases;

b) stored users' and employees' personal information on Chegg's network and databases, including S3 databases, in plain text, rather than encrypting the information;

c) used outdated and unsecure cryptographic hash functions to protect users' passwords;

d) failed to provide adequate guidance or training for employees or third-party contractors regarding information security and safeguarding users' and employees' personal information, including, but not limited to, failing to require employees to complete any data security training;

e) failed to develop, implement, or maintain adequate written organizational information security standards, policies, procedures, or practices;

f) failed to have a policy, process, or procedure for inventorying and deleting users' and employees' personal information stored on Chegg's network after that information is no longer necessary; and

g) failed to adequately monitor its networks and systems for unauthorized attempts to transfer or exfiltrate users' and employees' personal information outside of Chegg's network boundaries.[56]

[54] *In the Matter of CHEGG, INC., a corporation*, *supra* note 12.
[55] *Id.*
[56] *In the Matter of CHEGG, INC., a corporation*, *supra* note 12.

G. Chegg's Inadequate Data Security Caused Multiple Data Breaches

68. Chegg's failure to provide reasonable data security for the Sensitive Information it collected from customers has led to the repeated exposure of that personal information.

69. In approximately September 2017, Chegg employees fell for a phishing attack, giving the threat actors access to employees' direct deposit information. Prior to the hack, Chegg did not require employees to complete any data security training, including identifying and appropriately responding to phishing attacks; this failure contributed to the security incident.

70. Seven months later, in April 2018, a former contractor accessed one of Chegg's S3 databases using an AWS Root Credential. Although Amazon had provided public guidance to protect AWS Root Credentials "like you would your credit card numbers or any other sensitive secret" and that Amazon "strongly recommend[s] that you do not use the root user for your everyday tasks, even the administrative ones," Chegg shared the AWS Root Credentials among its employees and even outside contractors.[57] The former contractor exfiltrated a database containing personal information of approximately 40 million Chegg customers.

71. The exposed personal information included users' email addresses, first and last names, passwords, religious denomination, heritage, date of birth, parents' income range, sexual orientation, and disabilities. Chegg encrypted users' passwords using an outdated function that had been criticized by experts for years prior to April 2018.[58] Had Chegg employed reasonable access controls and monitoring, it would have likely detected and/or stopped the attack more quickly.

72. In approximately April 2019, a senior Chegg executive fell for a phishing attack, giving a hacker access to the executive's credentials to Chegg's email platform and exposing personal information about consumers and employees of Chegg. This executive's email system was in a default configuration state that allowed employees, as well as threat actors, to bypass Chegg's multifactor authentication requirement while accessing the email platform. The threat actor exploited this shortfall and gained access to the executive's email inbox, which contained the personal information of Chegg

[57] *In the Matter of CHEGG, INC., a corporation*, *supra* note 12.
[58] *Id.*

users and employees, including their financial and medical information.[59]

73. It is apparent that Chegg does not prioritize the security of its customers or employees. Indeed, in Chegg's 2021 Annual Report, it made the following statement: "efforts to prevent hackers from entering our computer systems are expensive to implement, may limit the functionality of our services, and we may need to expend significant additional resources to further enhance our safeguards and protection against security breaches or to redress problems caused by security breaches and such efforts may not be fully effective."[60]

74. Had Chegg properly configured its systems, including requiring multifactor authentication for employees to access their emails, this phishing attack, and the resulting exposure of consumer Sensitive Information, could have been prevented.

75. In addition, Chegg's failure to require employees to complete any data security training, including training to identify and respond to phishing attacks, contributed to the security incident.

76. Most recently, in April 2020, Chegg's senior employee responsible for payroll fell for a phishing attack, giving the threat actor access to the employee's credentials to Chegg's payroll system. The threat actor exfiltrated the W-2 information, including the birthdates and Social Security numbers, of approximately 700 current and former employees. Despite Chegg employees falling for phishing attacks on at least two prior occasions, Chegg still did not require, in or before April 2020, its employees to complete any data security training, including identifying and appropriately responding to phishing attacks.[61]

H. Chegg Knew It Needed to Protect Customers' Sensitive Information, But Did Not Protect that Information

77. Chegg knew the user data it collected and stored in connection with its services was highly sensitive.

78. From approximately March 2017 to January 2020, Chegg's privacy policy included the following language: "Chegg takes commercially reasonable security measures to protect the Personal

[59] *Id.*

[60] https://d18rn0p25nwr6d.cloudfront.net/CIK-0001364954/5ea8ad6f-677e-4b34-b835-ff01d33a2e9d.pdf.

[61] *In the Matter of CHEGG, INC., a corporation*, *supra* note 12.

Information submitted to us, both during transmission and once we receive it."[62] From January 2020 to the present, Chegg's privacy policy contained the following statement concerning that same personal information: "We take steps to ensure that your information is treated securely and in accordance with this Privacy Policy."[63] These statements indicate that Chegg was aware the sensitive and personal nature of the user data it stored.

79. Additionally, in a February 7, 2022 Press Release, Chegg included some "Forward Looking Statements." Within those statements, Chegg mentioned service disruptions related to cybersecurity and cyber-attacks twice throughout the statement, indicating that it was aware the potential for such threats.[64]

80. In February of 2022, Chegg submitted its 2021 Annual Report, in which Chegg anticipated repercussions for its lax data security and made the following statement: "Additionally, depending on the nature of the information compromised, in the event of a security breach or other privacy or security related incident, we may also have obligations to notify individuals and regulators about the incident, and we may need to provide some form of remedy, such as subscription credit monitoring services, payment of significant fines, or payment of compensation in connection with a class action settlement (including under the new-private right of action under the CCPA)."[65]

I. The Decryption of the Data Impacted by the Chegg Data Breaches

81. In an article published by Phil Hill, on PhilonEdTech, Mr. Hill explains that in September of 2019, the data exposed by the Chegg Data Breaches, prior to that date, had been decrypted (reversing the hash-based password encryption) and posted online, exposing student email and password combinations as described in an announcement from Tulane University IT:

> In 2018, Chegg.com, a company that offers textbook rental and tutoring services suffered a data breach resulting in the loss of 40 million customer records which included full names, email addresses, usernames, and passwords. Now the results of Chegg's 2018 data breach have been publicly exposed online, which poses a substantial threat. If users happen to reuse or slightly modify passwords across multiple services, publicly exposed

[62] *Id.*
[63] *Id.*
[64] *Chegg Investor Relations*, https://investor.chegg.com/Press-Releases/press-release-details/2022/Chegg-Reports-2021-Financial-Results-and-Gives-2022-Guidance/default.aspx.
[65] https://d18rn0p25nwr6d.cloudfront.net/CIK-0001364954/5ea8ad6f-677e-4b34-b835-ff01d33a2e9d.pdf (last visited Nov. 7, 2022).

credentials can be exploited.

> Several universities across the nation have reported malicious use of these leaked email addresses and passwords which were contained in the Chegg breach. This is of concern for anyone who may have signed up for Chegg using their Tulane email address and a password similar or identical to their Tulane.edu password. Several Tulane students and alumni have reached out to the IT service desk affected by this breach of Chegg data.[66]

82. Saint Mary's College described the discovery of the decryption as follows:

> [I]nformation obtained in the 2018 breach potentially included a Chegg user's name, email address, shipping address, Chegg username and hashed Chegg password. Saint Mary's College received a notification from REN-ISAC (Research and Education Networks Information Sharing and Analysis Center) 'that some credentials from your institution have appeared in a credential dump related to the Chegg data breach,'" Hausmann said in an email. "The information obtained from the Chegg data breach had been shared online for others to do further damage beyond the initial data breach of Chegg.[67]
>
> After hashed passwords are decrypted, the passwords can be used to sign into affected accounts if the passwords were not already changed," Hausmann said. "There is also the concern that the released e-mail addresses and passwords could be used to try and gain access into accounts unrelated to Chegg, including e-mail, social media and finance-related websites.[68]

83. The University of Central Florida made the following IT advisory announcement:

> According to a news alert sent by UCF INFOSEC Wednesday morning, the weak encryption used to store user data was the primary cause of cyber criminals gaining access to the information of thousands of users.[69]

J. Plaintiff's and the Class's Sensitive Information Has Value

84. The personal, health, and financial information of Plaintiff and the Class is valuable, intangible property. Indeed, it has market value to advertisers and cybercriminals seeking to obtain and use that information and the public and the marketplace values maintaining the privacy and confidentiality of individuals' Sensitive Information. Thus, Chegg was on notice of the need to implement reasonable data security measures.

85. Unlike financial information, like credit card and bank account numbers, the personal health information ("PHI") and certain PII exfiltrated in the Data Breach cannot be easily changed. Dates of birth and social security numbers are given at birth and attach to a person for the duration of his or

---

[66] Hill, Phil, Update on Chegg Data Breach, Decrypted credentials now leading to multiple campus security attacks, Philon EdTech, Nov. 25, 2019, https://philonedtech.com/update-on-chegg-data-breach-decrypted-credentials-now-leading-to-multiple-campus-security-attacks/.
[67] *Id.*
[68] *Id.*
[69] *Id.*

her life. For these reasons, these types of information are the most lucrative and valuable to hackers.[70]

86. Birth dates, Social Security numbers, addresses, employment information, income, and similar types of information can be used to open several credit accounts on an ongoing basis rather than exploiting just one account until it's canceled.[71]

87. In 2013, the Organization for Economic Cooperation and Development ("OECD") even published a paper entitled "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value."[72] In this paper, the OECD measured prices demanded by companies concerning user data derived from "various online data warehouses."[73]

88. OECD indicated that "[a]t the time of writing, the following elements of personal data were available for various prices: USD 0.50 cents for an address, USD 2 [i.e., $2] for a date of birth, USD 8 for a social security number (government ID number), USD 3 for a driver's license number and USD 35 for a military record. A combination of address, date of birth, social security number, credit record and military is estimated to cost USD 55."[74]

89. Consumers and businesses also place a considerable value on maintaining the privacy and confidentiality of their Sensitive Information. One 2002 study determined that U.S. consumers highly value a website's protection against improper access to their Sensitive Information, between $11.33 and $16.58 per website.[75] The study further concluded that to U.S. consumers, the collective "protection against error, improper access, and secondary use of personal information is worth between $30.49 and $44.62.[76] This data is approximately twenty years old, and the dollar amounts would likely

---

[70] *Calculating the Value of a Data Breach – What Are the Most Valuable Files to a Hacker?* Donnellon McCarthy Enters, https://www.dme.us.com/2020/07/21/calculating-the-value-of-a-data-breach-what-are-the-most-valuable-files-to-a-hacker/ (last visited Nov. 7, 2022).
[71] *Anthem hack: Personal data stolen sells for 10x Price of Stolen Credit Card Numbers*, Tim Greene, https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Jan. 18, 2022).
[72] Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, OECD Digital Economy Papers, NO. 220 (Apr. 2, 2013), https://www.oecdilibrary.org/docserver/5k486qtxldmq-en.pdf.
[73] *Id.* at 25.
[74] *Id.*
[75] 11-Horn Hann, Kai-Lung Hui, *et al*, *The Value of Online Information Privacy: Evidence from the USA and Singapore*, at 17. Marshall Sch. Bus., Univ. So. Cal. (Oct. 2002), https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (last visited Nov. 6, 2022).
[76] *Id.*

be exponentially higher today.

90. The FTC has also recognized that consumer data is a lucrative (and valuable) form of currency for businesses. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour underscored this point by reiterating that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable."[77] "Data is currency."[78]

91. When a data breach reveals Sensitive Information, it destroys the privacy and confidentiality of that data. Not only does that upset consumer expectations and wishes, but it also renders the data less valuable in the economy. Sensitive and personal "data has economic value" and can be used to further "artificial intelligence tools as well as the creation of intelligence targeting packages." Indeed, the integrity of Sensitive Information is material to individual's ability to prove their identity, which is necessary for individuals to obtain mortgages, credit cards, business loans; to submit tax returns; and to apply for a job. Consumers, likewise, exchange this type of information to businesses in exchange for goods, services, access, or discounts. Crucially, Minors may not be able to monitor the impact of the Data Breach on their lives for years, at which point the damage will be done and the minors will have to prove their identities.

92. When this information is released to cybercriminals and placed on the dark web, then individuals are less able to use that information to prove their identity because that information has been exposed to others willing or able to falsify and steal others' identities. Thus, the value of the breached information is lessened and its usefulness impaired.

93. Chegg's failure to provide reasonable data security for its users' Sensitive Information has caused and is likely to continue to cause substantial injury, including but not limited to identity theft, fraud, out-of-pocket monetary losses, decreased value of personal information, and time and effort spent remedying or attempting to prevent injuries, to those individuals whose data was exposed in breaches.

[77] Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable (Dec. 7, 2009), https://www.ftc.gov/news-events/news/speeches/remarks-ftc-exploring-privacy-roundtable (last visited Nov. 7, 2022).

[78] *Id.*

LEGAL BACKGROUND

A. Statute of Limitations (Tolling Under *American Pipe*)

94. While negligence claims are often covered by the two-year statute of limitations in California Code of Civil Procedure section 335.1, that statute addresses assault, battery, or physical injury. But the present action does not relate to assault, battery, or physical injury.

95. Because the gravamen of the negligence cause of action is breach of fiduciary duty, it likewise falls under the four-year catch-all statute of limitations. *See* Cal. Code Civ. Proc. § 343 ("An action for relief not hereinbefore provided for must be commenced within four years after the cause of action shall have accrued"); *Masimo Corp. v. True Wearables, Inc.*, 2022 WL 17083396 (C.D. Cal. Nov. 7, 2022) ("California applies a four-year statute of limitations to claims for breach of fiduciary duty").

96. The breach involving Plaintiff's information occurred in or around April 29, 2018, but Chegg did not disclose this until September 25, 2018.[79]

97. On September 10, 2019, Jabarri Lyles filed a nationwide class action in the Circuit Court of Baltimore City, Maryland against Defendant on behalf of "All persons residing in the United States, including the District of Columbia, whose PII was disclosed in the Chegg Data Breach." [80] The second cause of action was negligence.[81]

98. On November 8, 2019, the action was removed to the United States District Court for the District of Maryland. Shortly thereafter Defendant filed a motion to compel arbitration. On April 27, 2020, the district court granted the motion, dismissing the action without prejudice. *Lyles v. Chegg*, No. 1:19-cv-03235-RDB (D. Md. 2020), ECF No. 25. No motion for class certification was ever filed.

99. Under the United States Supreme Court precedent in *American Pipe & Construction v. Utah*, the statute of limitations for all nationwide class members was tolled during the pendency of the *Lyles* action. *See American Pipe*, 414 U.S. 538, 554 (1974) ("[T]he commencement of a class action suspends the applicable statute of limitation as to all asserted members of the class who would have been parties had the suit been permitted to continue as a class action").

---

[79] *Lyles v. Chegg, Inc.*, No. 24-C-19-004788, Compl., ECF No. 1-2, ¶ 3.
[80] *Id.* 1-2, at ¶ 52.
[81] *Id.* at ¶¶ 74-91.

100. As stated above, Plaintiff's negligence claim is governed by the four-year statute of limitations (i.e., 1461 days). Chegg first disclosed the breach on September 25, 2018, and the *Lyles* action was filed 350 days later. There were 925 days between the dismissal of the *Lyles* action and the filing of the present action. Between the 350 days before the *Lyles* action, and the 925 days after the *Lyles* action, there were 1,275 days between the breach being disclosed and the filing of the present action that were not tolled.

B. Accrual of the Action

101. "The date the statute commences is a '[c]ritical' aspect of the statute of limitations.'" *Baxter v. State Teachers Retirement Sys.*, 18 Cal. App. 5th 340, 358 (Cal. Ct. App. 2017) (citation omitted). "Typically, a party must bring suit within the specified time period after the claims accrues, meaning '"when [it] is complete with all its elements"—those elements being wrongdoing, harm, and causation.'" *Id.* (citation omitted).

102. In approximately September of 2019, the data from the breach was decrypted (reversing the hash-based password encryption) and posted online.[82] According to a Tulane University IT announcement, "If users happen to reuse or slightly modify passwords across multiple services, publicly exposed credentials can be exposed."[83]

103. According to the University of Central Florida Information Security Office, "the weak encryption used to store user data was the primary cause of cyber criminals gaining access to the information of thousands of users."[84]

104. As of November 25, 2019, Chegg had done nothing to notify users that their information had been decrypted and was available on the internet.[85] Moreover, Chegg never sent notice to Plaintiff that his data had been compromised and Plaintiff did not find out about the breach until 2022.

105. Plaintiff was injured by Defendant's data breach when his identity was stolen and his information was used to open a credit card. This occurred in October 2022, and Plaintiff reasonably

[82] Update on Chegg Data Breach: Decrypted credentials now leading to multiple campus security attacks, PHIL ON ED TECH (Nov. 25, 2019), *available at* https://philonedtech.com/update-on-chegg-data-breach-decrypted-credentials-now-leading-to-multiple-campus-security-attacks/.
[83] *Id.*
[84] *Id.*
[85] *Id.*

believes, based upon the information he has, that the only logically source of the identity theft and fraud is the Chegg Data Breaches.

106. Because the harm occurred in October 2022, the claim accrued in October 2022, when the final element of the claim occurred.

107. Plaintiff filed suit a month later.

C. Discovery Rule

108. "[T]he discovery rule is an exception to the general rule of accrual, 'postpon[ing] accrual of a cause of action until the plaintiff discovers, or has reason to discover, the cause of action." *Baxter*, 18 Cal.App.5th at 358 (citation omitted). "A plaintiff has reason to discover a cause of action when he or she '"has reason at least to suspect a factual basis for its elements,"' that is, the '"generic" element of wrongdoing, causation, and harm." *Id.* (citation omitted). "This is done '"to ameliorate a harsh rule that would allow the limitations period for filing suit to expire before a plaintiff has or should have learned of the latent injury and its cause."" *Id.*

109. Plaintiff was never informed of the data breach.

110. Chegg never provided him with any notice.

111. On September 25, 2018, Chegg made its first public disclosure of the data breach in its Form 8-K filing with the SEC.

112. Plaintiff does not read SEC filings, including Defendant's.

113. Plaintiff does not read Business Insider or Security Today, nor does he not watch CNBC. He never saw any news stories about the data breach.

114. Plaintiff does not visit the California Attorney General's website.

115. Because he was not informed of the breach, he had no reason to suspect, and therefore inquire, whether his information was lost by Chegg, and therefore search for Chegg data breaches.

116. Upon receiving notice of financial crimes being committed against him in October 2022 (i.e., harm), Plaintiff began a reasonable search for the cause. During that search, he learned of the data breaches.

117. Plaintiff filed this action a month later.

CLASS ALLEGATIONS

118. Plaintiff brings this action on behalf of himself and all other similarly situated Class members pursuant to Rule 23(a), (b)(2) and (b)(3) of the Federal Rules of Civil Procedure and seek certification of the following Nationwide Class and California Subclass:

Nationwide Class

All individuals whose data was impacted or otherwise compromised by one of, or any combination of the four, Chegg Data Breaches.

California Subclass

All California citizens whose data was impacted or otherwise compromised by one of, or any combination of the four, Chegg Data Breaches.

119. Together, the Nationwide Class and the California Subclass are the "Class" or the "Classes."

120. Excluded from the Class are Chegg and its subsidiaries and affiliates; all persons who make a timely election to be excluded from the class; government entities; and the judge to whom this case is assigned and his/her immediate family and court staff.

121. Plaintiff reserves the right to, after conducting discovery, modify, expand, or amend the above Class definition or to seek certification of a class or Classes defined differently than above before any court determines whether certification is appropriate.

122. **Numerosity**. Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that joinder of all Class members is impracticable. Plaintiff believes that there are millions of members of the Class. The number of reportedly impacted individuals already exceeds forty (40) million, and Plaintiff believes additional entities and persons may have been affected by the Data Breaches. The precise number of class members, however, is unknown to Plaintiff. Class members may be identified through objective means. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

123. **Commonality and Predominance**. Consistent with Fed. R. Civ. P. 23(a)(2) and with 23(b)(3)'s commonality and predominance requirements, this action involves common questions of law

and fact which predominate over any questions affecting individual Class members. These common questions include, without limitation:

a. Whether Chegg knew or should have known that its data environment and cybersecurity measures created a risk of a data breach;

b. Whether Chegg controlled and took responsibility for protecting Plaintiff's and the Class's data when solicited that data, collected it, and stored it on its servers;

c. Whether Chegg's security measures were reasonable considering the FTC data security recommendations, state laws and guidelines, industry standards, and common recommendations made by data security experts;

d. Whether Chegg owed Plaintiff and the Class a duty to implement reasonable security measures;

e. Whether Chegg's failure to adequately secure Plaintiff's and the Class's data constitutes a breach of its duty to institute reasonable security measures;

f. Whether Chegg's failure to implement reasonable data security measures allowed the breach of its data systems to occur and caused the theft of Plaintiff's and the Class's data;

g. Whether reasonable security measures known and recommended by the data security community could have prevented the breach;

h. Whether Plaintiff and the Class were injured and suffered damages or other losses because of Chegg's failure to reasonably protect its data systems; and

i. Whether Plaintiff and the Class are entitled to relief.

124. **Typicality**. Consistent with Fed. R. Civ. P. 23(a)(3), Plaintiff is a typical member of the Class. Plaintiff and the members of the Class are persons whose provided data to Chegg, whose data resided on Chegg's servers, and whose personally identifying information was exposed in Chegg's Data Breaches. Plaintiff's injuries are like other class members and Plaintiff seeks relief consistent with the relief due to the Class.

125. **Adequacy**. Consistent with Fed. R. Civ. P. 23(a)(4), Plaintiff is an adequate representative of the Class because Plaintiff is a member of the Class and is committed to pursuing this matter against Chegg to obtain relief for himself and for the Class. Plaintiff has no conflicts of interest with the Class. Plaintiff has also retained counsel competent and experienced in complex class action litigation of this type, having previously litigated data breach cases. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

126. **Superiority**. Consistent with Fed. R. Civ. P 23(b)(3), class action litigation is superior

to any other available means for the fair and efficient adjudication of this controversy. Individual litigation by each Class member would strain the court system because of the numerous members of the Class. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court. A class action would also permit customers to recover even if their damages are small as compared to the burden and expense of litigation, a quintessential purpose of the class action mechanism.

127. **Injunctive and Declaratory Relief**. Consistent with Fed. R. Civ. P. 23(b)(2), Defendant, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the class as a whole.

LEGAL CLAIMS

COUNT I
Negligence
(on behalf of the Nationwide Class, or alternatively the California Subclass)

128. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

129. Plaintiff brings this claim for negligence against Chegg on behalf of the Nationwide Class. Alternatively, Plaintiff brings this claim on behalf of the California Subclass.

130. Chegg owed a duty to Plaintiff and the members of the Class to take reasonable care in managing and protecting the sensitive data it solicited from Plaintiff and the Class and managed and stored. This duty arises from multiple sources.

131. Chegg owed a common law duty to Plaintiff and the Class that existed outside of any contractual agreement or Terms of Use to implement reasonable data security measures because it was foreseeable that hackers would target Chegg's data systems and servers containing Plaintiff's and the Class's sensitive data and that, should a breach occur, Plaintiff and the Class would be harmed. Chegg alone controlled its technology, infrastructure, and cybersecurity. It further knew or should have known that if hackers breached its data systems, they would extract sensitive data and inflict injury upon Plaintiff and the Class. Furthermore, Chegg knew or should have known that if hackers accessed the

sensitive data, the responsibility for remediating and mitigating the consequences of the breach would largely fall on individual persons whose data was impacted and stolen. Therefore, the Data Breaches, and the harm it caused Plaintiff and the Class, was the foreseeable consequence of Chegg's unsecured, unreasonable data security measures.

132. Additionally, Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, required Chegg to take reasonable measures to protect Plaintiff's and the Class's sensitive data and is a further source of Chegg's duty to Plaintiff and the Class. Section 5 prohibits unfair practices in or affecting commerce, including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like Chegg of failing to use reasonable measures to protect sensitive data. Chegg, therefore, was required and obligated to take reasonable measures to protect data it possessed, held, or otherwise used. The FTC publications and data security breach orders described herein further form the basis of Chegg's duty to adequately protect sensitive information. By failing to implement reasonable data security measures, Chegg acted in violation of § 5 of the FTCA.

133. Chegg is obligated to perform its business operations in accordance with industry standards. Industry standards are another source of duty and obligations requiring Chegg to exercise reasonable care with respect to Plaintiff and the Class by implementing reasonable data security measures that do not create a foreseeable risk of harm to Plaintiff and the Class.

134. Chegg breached its duty to Plaintiff and the Class by implementing unreasonable data security measures that it knew or should have known could cause a Data Breach. Chegg knew or should have known that hackers might target sensitive data that Chegg solicited and collected on its users and, therefore, needed to use reasonable data security measures to protect against a Data Breach. Indeed, Chegg acknowledged it was subject to certain standards to protect data and utilize other industry standard data security measures. Chegg, furthermore, represented to users that their data was safe with Chegg.

135. Chegg was fully capable of preventing the Data Breaches. Chegg, as a smart technology-based company, knew or should have known of data security measures required or recommended by the FTC, state laws and guidelines, and other data security experts which, if implemented, would have prevented the Data Breaches from occurring at all, or limited and shortened the scope of the Data

Breaches. Chegg thus failed to take reasonable measures to secure its system, leaving it vulnerable to a breach.

136. As a direct and proximate result of Chegg's negligence, Plaintiff and the Class have suffered and will continue to suffer injury, including the ongoing risk that their data will be used nefariously against them or for fraudulent purposes.

COUNT II
Negligence *Per Se*
(on behalf of the Nationwide Class, or alternatively the California Subclass)

137. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

138. Plaintiff brings this claim for negligence *per se* against Chegg on behalf of the Nationwide Class. Alternatively, Plaintiff brings this claim on behalf of the California Subclass.

139. Chegg's unreasonable data security measures and constitute unfair or deceptive acts or practices in or affecting commerce in violation Section 5 of the FTC Act.[86] Although the FTC Act does not create a private right of action, both require businesses to institute reasonable data security measures and breach notification procedures, which Chegg failed to do.

140. Section 5 of the FTCA, 15 U.S.C. § 45, prohibits "unfair. . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like Chegg of failing to use reasonable measures to protect users' sensitive data. The FTC's complaint against Chegg also forms the basis of Chegg's duty.[87]

141. Chegg violated Section 5 of the FTC Act by failing to use reasonable measures to protect users' personally identifying information and sensitive data and by not complying with applicable industry standards. Chegg's conduct was particularly unreasonable given the sensitive nature and amount of data it stored on its users and the foreseeable consequences of a Data Breach should Chegg fail to secure its systems.

142. Chegg's violation of Section 5 of the FTC Act constitutes negligence per se.

143. Plaintiff and the Class are within the class of persons Section 5 of the FTCA (and similar

[86] *In the Matter of CHEGG, INC., a corporation*, *supra* note 12.
[87] *Id.*

state statutes) was intended to protect. Additionally, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. The FTC has pursued over fifty enforcement actions against businesses which, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same type of harm suffered by Plaintiff and the Class.

144. As a direct and proximate result of Chegg's negligence per se, Plaintiff and the Class have suffered and continue to suffer injury.

COUNT III

Violation of California's Consumers Legal Remedies Act, Cal. Civ. Code § 1750 *et seq.*

(on behalf of the Nationwide Class, or alternatively the California Subclass)

145. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

146. Plaintiff brings this claim for violation of California's Consumers Legal Remedies Act, Cal. Civ. Code § 1750 *et seq.* ("CLRA"), against Chegg on behalf of the Nationwide Class. Alternatively, Plaintiff brings this claim on behalf of the California Subclass.

147. The CLRA is liberally construed to protect consumers against unfair and deceptive business practices in connection with the conduct of businesses providing goods, property or services to consumers primarily for personal, family, or household use.

148. Chegg is a "person" as defined by the CLRA, and it provided "services" as defined under the act. Cal. Civ. Code §§ 1761(b)-(c), 1770.

149. The CLRA prohibits a defendant who is involved in a transaction from "[r]epresenting that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have." § 1770(a)(5).

150. Additionally, the CLRA prohibits a defendant who is involved in a transaction from "[r]epresenting that goods or services are of a particular standard, quality, or grade . . . if they are of another." § 1770(a)(7).

151. Plaintiff Keller and the Class members are "consumer[s]" as who were engaged in a "transaction" under the act. §§ 1761(d)-(e), 1770.

152. Chegg's acts and practices were intended to and did result in the sales of services to

Plaintiff and the Class members in violation of California Civil Code § 1770, including, but not limited to, the following:

a. Implementing and maintaining cybersecurity and privacy measures that were knowingly insufficient to protect Plaintiff Keller's and the Classes' sensitive data, which was a direct and proximate cause of the Data Breaches;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breaches;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Keller's and Class members' sensitive data, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breaches;

d. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff Keller's and Class members' sensitive data; and

e. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Keller's and Class members' sensitive data, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45.

153. Chegg's omissions were material because they were likely to and did deceive reasonable consumers about the adequacy of Chegg's data security and ability to protect the confidentiality of consumers' sensitive information that Chegg solicited, collected, and stored.

154. Had Chegg disclosed, rather than concealing, to Plaintiff and class members that their cybersecurity, digital platforms, and data storage systems were not secure and, thus, vulnerable to attack, Chegg would have been unable to continue in business and would have been forced to adopt reasonable data security measures and comply with the law.

155. Instead, Chegg received, maintained, and compiled Plaintiff's and class members' sensitive data as part of the services Chegg provided and for which Plaintiff and Class members paid, in part, through transaction fees by (1) omitting and concealing information from Plaintiff Keller and Class members that Chegg's data security practices were knowingly insufficient to maintain the safety and confidentiality of Plaintiff's and class members' sensitive data and (2) that Chegg was not compliant with basic data security requirements and best practices to prevent a Data Breach. Accordingly, Plaintiff Keller and the Class members acted reasonably in relying on Chegg's omissions, the truth of which they could not have discovered.

156. On information and belief, Chegg's actions were willful, wanton, and fraudulent.

157. On information and belief, officers, directors, or managing agents at Chegg authorized the actions discussed above.

158. On November 8, 2022, Plaintiff Keller and the Class sent notice to Chegg in compliance with California Civil Code section 1782(a) via certified mail. Chegg has not complied with the California Civil Code section 1782(a) notice. Plaintiff and the other Class members seeks injunctive relief, reasonable attorney fees and costs, restitution, damages, and any other relief that the Court deems proper.

COUNT IV
Violation of the California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 *et seq.*
(on behalf of the Nationwide Class, or alternatively the California Subclass)

159. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

160. Plaintiff brings this claim for violation of the California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 *et seq.*, against Chegg on behalf of the Nationwide Class. Alternatively, Plaintiff brings this claim on behalf of the California Subclass.

161. Chegg is a corporation organized or operated for the profit or financial benefit of its owners with annual net revenues over $776.3 million in 2021 and between $830 and $850 million in 2022.[88]

162. Chegg collects and stores consumers' personal information, including sensitive and personal information, as defined by California Civil Code section 1798.81.5.

163. Chegg had a duty to implement and maintain reasonable security procedures and practices to protect Plaintiff Keller's and members of the Class's sensitive and personal data.

164. Chegg failed to meet its duty, resulting in unauthorized access and exfiltration, theft, or disclose of Plaintiff Keller's, and the Class's, personal and sensitive data in violation of California Civil Code section 1798.150.

165. Plaintiff Keller and members of the Class seek relief pursuant to section 1798.150(a),

[88] *Chegg Investor Relations*, *supra* note 64.

including *inter alia*, actual damages, injunctive relief, and any other relief this Court deems proper. Plaintiff Keller and the Class also seek attorneys' fees and costs pursuant to California Code of Civil Procedure section 1021.5. Plaintiff does not seek statutory damages in this complaint.

166. On November 8, 2022, Plaintiff Keller and the Class sent notice to Chegg in compliance with California Civil Code section 1798.150(b) via certified mail. Defendant did not comply with the notice. Accordingly, Plaintiff and the other members of the Class seek statutory damages, actual damages and injunctive relief in this complaint.

167. Because Chegg is still in possession of Plaintiff Keller's, and the other members of the Class's, sensitive and personal data, Plaintiff Keller seek statutory damages as well as injunctive or other equitable relief to ensure that Chegg implements and maintains reasonable data security measures and practices to prevent an event like the Data Breach from occurring again.

COUNT V
Violation of California's False Advertising Law, Cal. Bus. & Prof. Code § 17500 *et seq.*
(on behalf of the Nationwide Class, or alternatively the California Subclass)

168. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

169. Plaintiff brings this claim for violation of California's False Advertising Law, Cal. Bus. & Prof. Code § 17500 *et seq.* ("FAL"), against Chegg on behalf of the Nationwide Class. Alternatively, Plaintiff brings this claim on behalf of the California Subclass.

170. The FAL provides that "[i]t is unlawful for any person, firm, corporation or association, or any employee thereof with intent directly or indirectly to dispose of real or personal property or to perform services" to disseminate any statement "which is untrue or misleading, and which is known, or which by the exercise of reasonable care should be known, to be untrue or misleading." Cal. Bus. & Prof. Code § 17500.

171. It is also unlawful under the FAL to disseminate statements concerning property or services that are "untrue or misleading, and which is known, or which by the exercise of reasonable care should be known, to be untrue or misleading." *Id.*

172. As alleged herein, since at least 2017, Chegg's privacy policy contained the following representation regarding the security measures Chegg used to protect the personal information it

collected from users: "Chegg takes commercially reasonable security measures to protect the Personal Information submitted to us, both during transmission and once we receive it."

173. Chegg's representations are false and misleading because the Data Breaches show that Chegg ***does not*** take commercially reasonable security measures to protect the PII of Plaintiff and California Class Members who purchase and use Chegg's educational products and services.

174. Chegg has represented, directly or indirectly, expressly or by implication, that it implemented reasonable measures to protect personal information against unauthorized access.

175. Chegg's representations misled consumers acting reasonably.

176. Plaintiff Keller and the Class members suffered injuries due to Chegg's actions as set forth herein because Chegg did not take commercially reasonable security measures to protect Plaintiff and Class members' PII, as evidenced by multiple Data Breaches.

177. Chegg's business practices as alleged herein constitute deceptive, untrue, and misleading advertising pursuant to the FAL because Chegg has advertised the security of its systems in a manner that is untrue and misleading, which Defendant knew or reasonably should have known, and omitted material information from its privacy policy or any other advertising for Chegg's education products and services.

178. Chegg profited from selling to unwary consumers falsely and deceptively advertised educational products and services and the security of consumers' information necessary to obtain Chegg's products and services.

179. Plaintiff Keller and the Class members were damaged because they would not have used for Chegg's educational products and services had they known the true facts regarding Chegg's security measures and that Chegg's security measures were inadequate, thereby exposing Plaintiff Keller and the Class members' PII to cyber criminals as a result of the Data Breaches.

180. Plaintiff Keller and the Class members do not have an adequate remedy at law because damages alone will not stop Chegg's unlawful conduct alleged herein. Damages will only address past injuries visited on Plaintiff Keller and the Class members. Only injunctive relief can prevent any future harm. Additionally, legal damages may not be available to Plaintiff. Indeed, restitution under the FAL can be awarded in situations where the entitlement to damages may prove difficult. *Cortez v. Purolator*

Air Filtration Products Co., 23 Cal. 4th 163, 177 (2000) (Restitution can be awarded "even absent individualized proof that the claimant lacked knowledge of the overcharge when the transaction occurred."); *see also Gutierrez v. Wells Fargo Bank, NA*, 589 F. App'x 824, 827 (9th Cir. 2014) (same); *In re Steroid Hormone Prod.*, 181 Cal. App. 4th 145, 156-57 (2010) (Plaintiff was entitled to show that defendant's deceptive conduct caused damages uniform to the class even if some class members would have purchased the products in question if they were aware of defendant's business practices.); *Caro v. Procter & Gamble Co.*, 18 Cal. App. 4th 644, 661 (1993) (The court "is empowered to grant equitable relief, including restitution in favor of absent persons, without certifying a class action.").

181. But even if damages were available, such relief would not be adequate to address the injury suffered by Plaintiff Keller and the Class members. Unlike damages, the Court's discretion in fashioning equitable relief is very broad. *Cortez*, 23 Cal. 4th at 180. Thus, restitution would allow recovery even when normal consideration associated with damages would not. *See, e.g., Fladeboe v. Am. Isuzu Motors Inc.*, 150 Cal. App. 4th 42, 68 (2007) (noting that restitution is available even in situations where damages may not be available).

182. As a result, Plaintiff Keller and the Class members seek equitable relief, an injunction, restitution, and an order for the disgorgement of the funds by which Chegg was unjustly enriched.

COUNT VI
Violations of California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 *et seq.*
(on behalf of the Nationwide Class, or alternatively the California Sub-Class)

183. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

184. Plaintiff brings this claim for California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 *et seq.* ("UCL"), against Chegg on behalf of the Nationwide Class. Alternatively, Plaintiff brings this claim on behalf of the California Subclass.

185. Chegg is a "person" as defined by California Business and Professions Code section 17201.

186. Chegg violated the UCL by engaging in unlawful, unfair, and deceptive business acts and practices.

187. Chegg's unlawful, unfair acts and deceptive acts and practices include:

a. Chegg's failure to employ reasonable and appropriate measures to protect personal information caused or is likely to cause substantial injury to consumers that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers themselves. This practice is an unfair act or practice, which was a direct and proximate cause of the Data Breaches;

b. Chegg implementing and maintaining cybersecurity and privacy measures that were knowingly insufficient to protect Plaintiff Keller's and the Class members' sensitive data, which was a direct and proximate cause of the Data Breaches;

c. Chegg's failure to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breaches;

d. Chegg's failure to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Keller's and Class members' sensitive data, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breaches;

e. Chegg's omission, suppression, and concealment of material facts that it did not reasonably or adequately secure Plaintiff Keller's and Class members' sensitive data;

f. Chegg's omissions, suppression, and concealment of the material facts that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Keller's and Class members' sensitive data, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45;

g. Chegg's failure to implement and maintain reasonable security measures also led to substantial injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because Plaintiff Keller and the Class members could not know of Chegg's inadequate security, consumers could not have reasonably avoided the harms that Chegg caused;

h. Chegg misrepresented that it would protect the privacy and confidentiality of Plaintiff Keller and the Class members' PII, including by implementing and maintaining reasonable security measures;

i. Chegg misrepresented that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Keller and the Class members' PII, including duties imposed by the FTCA, 15 U.S.C § 45; California Civil Code section 1798.150 *et seq.*; and California Civil Code section 1750;

j. Chegg engaged in unlawful business practices by violating the FAL as described in Count V;

k. Chegg engaged in unlawful business practices by violating California Civil Code section 1798.82; and

l. Among other ways to be discovered and proved at trial.

188. Chegg could have prevented or mitigated these information security failures through readily available, and relatively low-cost, measures, including, for example, encryption keys.

189. Chegg's representations and omissions to Plaintiff Keller and the Class members were material because they were likely to deceive reasonable consumers about the adequacy of Chegg's data security and ability to protect the privacy of consumers' PII.

190. Chegg intended to mislead Plaintiff Keller and the Class members and induce them to rely on its misrepresentations and omissions.

191. Had Chegg disclosed to Plaintiff Keller and the Class members that its data systems were not secure and, thus, vulnerable to attack, Chegg would have been unable to continue in business, and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Chegg received, maintained, and compiled Plaintiff Keller's and the Class members' PII as part of the services and goods Chegg provided without advising Plaintiff Keller and the Class members that Chegg's data security practices were insufficient to maintain the safety and confidentiality of Plaintiff Keller and the Class members. Accordingly, Plaintiff Keller and the Class members acted reasonably in relying on Chegg's misrepresentations and omissions, the truth of which they could not have discovered.

192. Chegg acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff Keller and the Class members' rights.

193. As a direct and proximate result of Defendant's unfair, unlawful, and fraudulent acts and practices, Plaintiff Keller and the Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages as described herein and as will be proved at trial.

194. Plaintiff Keller and the Class members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Chegg's unfair, unlawful, and fraudulent business practices or use of their PII; declaratory relief; injunctive relief; reasonable attorneys' fees and costs under California Code of Civil Procedure section 1021.5; and other appropriate equitable relief.

195. Plaintiff Keller and the Class members do not have an adequate remedy at law because damages alone will not stop Chegg's unlawful conduct alleged herein. Damages will only address past injuries visited on Plaintiff Keller and the Class members. Only injunctive relief can prevent any future harm. Additionally, legal damages may not be available to Plaintiff.

196. Plaintiff Keller and the Class members do not have an adequate remedy at law because damages alone will not stop Chegg's unlawful conduct alleged herein. Damages will only address past injuries visited on Plaintiff Keller and the Class members. Only injunctive relief can prevent any future harm. Additionally, legal damages may not be available to Plaintiff. Indeed, restitution under the UCL can be awarded in situations where the entitlement to damages may prove difficult. *Cortez*, 23 Cal. 4th at 177 (Restitution under the UCL can be awarded "even absent individualized proof that the claimant lacked knowledge of the overcharge when the transaction occurred."); *Gutierrez*, 589 F. App'x at 827 (same); *Caro*, 18 Cal. App. 4th at 661 (The court "is empowered to grant equitable relief, including restitution in favor of absent persons, without certifying a class action.").

197. But even if damages were available, such relief would not be adequate to address the injury suffered by Plaintiff Keller and the Class members. Unlike damages, the Court's discretion in fashioning equitable relief is very broad. *Cortez*, 23 Cal. 4th at 180. Thus, restitution would allow recovery even when normal consideration associated with damages would not. *See, e.g.*, *Fladeboe v. Am. Isuzu Motors Inc.*, 150 Cal. App. 4th 42, 68 (2007) (noting that restitution is available even in situations where damages may not be available).

198. As a result, Plaintiff Keller and the Class members are entitled to equitable relief, injunction, restitution, and an order for the disgorgement of the funds by which Chegg was unjustly enriched.

COUNT VII
Declaratory and Injunctive Relief
(on behalf of the Nationwide Class, or alternatively the California Sub-Class)

199. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

200. Under the Declaratory Judgment Act, 28 U.S.C. § 2201 *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those alleged herein, which are tortious, and which violate the terms of the federal and state statutes described above.

201. An actual controversy has arisen in the wake of the Data Breaches at issue regarding Defendant's common law and other duties to act reasonably with respect to safeguarding the data of

Plaintiff and the Class. Plaintiff alleges Chegg's actions in this respect were inadequate and unreasonable and, upon information and belief, remain inadequate and unreasonable. Additionally, Plaintiff and the Class continue to suffer injury due to the continued and ongoing threat of additional fraud against them or on their accounts.

202. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Chegg owed, and continues to owe a legal duty to secure the sensitive information with which it is entrusted, specifically including information it obtains from its customers, and to notify impacted individuals of the Data Breach under the common law, Section 5 of the FTC Act;

b. Chegg breached, and continues to breach, its legal duty by failing to employ reasonable measures to secure its customers' personal information; and

c. Chegg's breach of its legal duty continues to cause harm to Plaintiff and the Class.

203. The Court should also issue corresponding injunctive relief requiring Chegg to employ adequate security protocols consistent with industry standards to protect its users' and employees' (*i.e.*, Plaintiff's and the Class's) data.

204. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another breach of Chegg's data systems. If another breach of Chegg's data systems occurs, Plaintiff and the Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiff and the Class for their out-of-pocket and other damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiff and the Class, which include monetary damages that are not legally quantifiable or provable.

205. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the hardship to Chegg if an injunction is issued.

206. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the injuries that would result to Plaintiff, the Class, and the public at large.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Class, requests that this Court award relief as follows:

a. An order certifying the class and designating Plaintiff as the Class Representative and his counsel as Class Counsel;

b. An award to Plaintiff and the proposed Class members of damages with pre-judgment and post-judgment interest;

c. A declaratory judgment in favor of Plaintiff and the Class;

d. Injunctive relief to Plaintiff and the Class;

e. An award of attorneys' fees and costs as allowed by law; and

f. An award such other and further relief as the Court may deem necessary or appropriate.

JURY TRIAL DEMANDED

Plaintiff hereby demands a jury trial for all the claims so triable.

Date: February 3, 2023

REESE LLP

/s/ Michael R. Reese
Michael R. Reese (Cal. State Bar No. 206773)
mreese@reesellp.com
Sue J. Nam (Cal. State Bar No. 206729)
snam@reesellp.com
100 West 93rd Street, 16th Floor
New York, New York 10025
Telephone: (212) 643-0500

REESE LLP
George V. Granade (Cal. State Bar No. 316050)
ggranade@reesellp.com
8484 Wilshire Boulevard, Suite 515
Los Angeles, California 90211
Telephone: (310) 393-0070

REESE LLP
Charles D. Moore (admitted *pro hac vice*)
cmoore@reesellp.com
100 South 5th Street, Suite 1900
Minneapolis, Minnesota 55402
Telephone: (212) 643-0500

ZIMMERMAN REED LLP
Brian C. Gudmundson (admitted *pro hac vice*)
bgudmundson@zimmreed.comv
Rachel K. Tack (admitted *pro hac vice*)
rachel.tack@zimmreed.com
Michael J. Laird (admitted *pro hac vice*)
michael.laird@zimmreed.com
1100 IDS Center
80 South 8th Street
Minneapolis, Minnesota 55402
Telephone: (612) 341-0400

LAUKAITIS LAW FIRM LLC
Kevin Laukaitis (*pro hac vice* pending)
klaukaitis@laukaitislaw.com
737 Bainbridge Street, Suite 155
Philadelphia, Pennsylvania 19147
Telephone: (215) 789-4462

Counsel for Plaintiff Joshua Keller and the Proposed Class